Jehan A. Patterson
Julie A. Murray
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000
jpatterson@citizen.org

Attorneys for Amici Curiae
Public Citizen, Inc. and
Chris Jay Hoofnagle

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION Plaintiff, v. WYNDHAM WORLDWIDE CORPORATION, *et al.*, Defendants.	Civil Action No. 13-cv-01887-ES-SCM **PROPOSED AMICI CURIAE BRIEF OF PUBLIC CITIZEN, INC. AND CHRIS JAY HOOFNAGLE IN SUPPORT OF PLAINTIFF FEDERAL TRADE COMMISSION'S OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS** Return Date: June 17, 2013 (by court order dated May 14, 2013)

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Civil Procedure 7.1, amicus curiae Public Citizen, Inc. states that it has no parent corporation and that there is no publicly held corporation that owns 10% or more of Public Citizen, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

ADMINISTRATIVE MATERIALS

MISCELLANEOUS

INTERESTS OF AMICI CURIAE

Public Citizen, Inc., a non-profit advocacy organization with more than 300,000 members and supporters nationwide, appears before Congress, federal agencies, and the courts to advocate for consumer protections, government transparency, access to courts, and health and safety regulations. Since its founding more than forty years ago, Public Citizen has appeared frequently as a party or amicus curiae in cases around the country to advocate for increased consumer protections and stronger regulatory authority across a variety of industries, including in *Federal Trade Commission v. Watson Pharmaceuticals, Inc.*, No. 12-416 (U.S. filed Jan. 29, 2013) (counsel for amicus curiae supporting Federal Trade Commission (FTC) antitrust action concerning anti-competitive deals between brand-name and generic drug manufacturers); *In re Ameritrade Accountholder Litigation*, 266 F.R.D. 418, 419 (N.D. Cal. 2009) (counsel for objector/class member in case arising out of data breach that exposed consumer information); and *Lee v. Carter-Reed Co., LLC*, 4 A.3d 561, 566 (N.J. 2010) (amicus curiae in case alleging New Jersey Consumer Fraud Act and common-law claims against dietary supplement manufacturer). The theft of consumers' personal information from a company's computer network significantly increases the risk that those consumers will become victims of identity fraud and suffer substantial injuries. Regulatory enforcement against companies that fail to reasonably protect the security of their

computer systems, thus rendering their systems vulnerable to breaches in which consumer data can be stolen, is critical as corporate data breaches continue to increase.

Chris Jay Hoofnagle is a lecturer in residence at the University of California, Berkeley School of Law, where he teaches courses on the FTC's regulation of privacy and on computer crime law. In a series of articles published at Stanford, UCLA, Loyola, and Harvard, Mr. Hoofnagle established identity theft as an externality flowing from the economic incentives in credit granting and accepting relationships, and he proposed mechanisms to internalize the costs of fraud among these information-intensive businesses. He has testified before Congress and at FTC events numerous times concerning identity theft and privacy law.

All parties have consented to the filing of this brief. No counsel for any party authored this brief in whole or part. Apart from amici, no person, including parties or parties' counsel, contributed money intended to fund the preparation and submission of this brief.

SUMMARY OF ARGUMENT

As consumers transact more business online, they entrust significant amounts of sensitive information—financial, medical, and other personal data, such as birthdates and even Social Security numbers—to the companies with

which they do business. Recognizing the value of such consumer information, criminals seek to exploit vulnerabilities in companies' computer systems.

Sensitive consumer data such as credit or debit card numbers, bank account information, and Social Security numbers command large sums on the black market, as criminals can use this information to drain funds from bank accounts, make fraudulent purchases, apply for credit, and wrongfully obtain tax refunds or other government benefits. When such information is stolen, consumers expend money and time to, for example, dispute fraudulent transactions, notify their creditors of the identity fraud, and repair their credit. In more extreme (but not necessarily uncommon) instances, consumers may be denied employment because of a damaged credit report, be unable to obtain low-cost credit, or be denied access to credit entirely, impairing their chances of purchasing a home or financing an education.

Although the injuries resulting from a data breach can be significant, private tort suits alleging such injuries are nascent, and federal courts to date have not recognized a private remedy against companies whose networks are breached for consumers whose data is stolen but not yet misused. Thus, FTC enforcement actions pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, against companies that fail to reasonably protect their consumers' information from misappropriation are currently the key means of protecting consumers. Indeed, FTC enforcement

actions such as the one at issue here have served as the only effective means of redressing the unfair corporate practices that lead to corporate data breaches that cause substantial injuries to consumers.

ARGUMENT

I. CONSUMERS SUFFER SUBSTANTIAL HARM FROM THEFT OF THEIR FINANCIAL AND PERSONAL DATA.

A. Sensitive Consumer Information Is at Risk of Theft from Corporate Data Breaches.

Recent years have seen a number of high-profile corporate data breaches involving millions of compromised consumer records.[1] An annual study by the Verizon RISK team, in tandem with national and international law enforcement agencies, data security researchers, and forensic auditors, confirmed 621 data breaches and approximately 44 million compromised data records in 2012 alone. Verizon, *2013 Data Breach Investigations Report* 11.[2]

Hackers who breach corporate computer networks or websites to steal consumer data do not necessarily exploit the information themselves by making fraudulent purchases or applying for credit. Instead, consumer information is

[1] *See* Jordan Robertson, *Customers Stay Despite High-Profile Data Breaches*, USA Today, May 2, 2011, http://usatoday30.usatoday.com/tech/news/2011-05-02-online-privacy_n.htm; *see also* Privacy Rights Clearinghouse, *Data Breaches: A Year in Review*, Dec. 16, 2011, https://www.privacyrights.org/data-breach-year-review-2011.

[2] The full report is available for download at http://www.verizonenterprise.com/DBIR/2013/.

bought and sold in bulk, as "[t]he most successful identity thieves have learned that it's more lucrative to hack into businesses, where they can steal card numbers by the thousands or even millions," with each credit card number fetching a sale price of anywhere from ten to several hundred dollars.[3] Because the "crime profits [from data theft] can be staggering,"[4] attacks on corporate computer networks show no signs of abating.

B. The Fraudulent Use of Consumer Information Causes Significant Harm to Consumers.

The consequences of misappropriated consumer information are wide-ranging and extend far beyond the inconvenience of a cancelled credit card. One in four consumers who were notified by a company that their data was stolen became a victim of identity fraud in 2012.[5] Indeed, identity fraud has become the top consumer complaint to the FTC.[6]

---

[3] J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA Today, Apr. 14, 2013, http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179.

[4] Greg Farrell & Michael A. Riley, *Hackers Take $1 Billion a Year As Banks Blame Their Clients*, Bloomberg, Aug. 4, 2011, http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html.

[5] Javelin Strategy & Research, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, https://www.javelinstrategy.com/brochure/276.

[6] FTC, *Consumer Sentinel Network Data Book for January – December 2012*, at 3, Feb. 2013, http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

Consumers experience direct economic and opportunity costs in attempting to avoid identity theft. Proactive consumers who wish to prevent fraudulent use of their information upon learning of a data breach may place a freeze on their credit reports to prevent prospective creditors from accessing their reports or credit scores without permission, but with a freeze in place, they are themselves unable to obtain immediate credit, such as store credit cards.[7] Further, consumers whose information has been stolen are more likely to purchase credit card insurance or credit repair services. Jason Fitterer, *Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-Mail Receipts*, 9 Nw. J. Tech. & Intellectual Prop. 591, 9 (2011) (estimating that consumers spend approximately $7.5 billion annually on these products and services). And for those consumers whose credit or debit card information is used in fraudulent transactions, the "loss of time in dealing with problems associated with [the misuse] such as bounced checks, loan denials, credit card application rejections, debt collection harassment, insurance rejections, and the shut-down of utilities" is significant. S. Jacob Carroll, *FAA v. Cooper: Bombarding the Privacy Act with the "Canon of Sovereign Immunity,"* 64 Mercer L. Rev. 785, 804 (2013) (internal quotation marks and citation omitted).

[7] Identity Theft Resource Center, *ITRC Fact Sheet 124 – Fraud Alerts and Credit Freezes*, July 10, 2010, http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_124_Credit_Freezes_and_Fraud_Alerts.shtml.

Even data breaches where only names and email addresses are stolen can be harmful, as the information may be used to probe for more data on those consumers, thus increasing the likelihood that the consumers will be targeted for a phishing scheme that may lead to identity fraud. In phishing schemes, a "perpetrator will provide an e-mail or link that directs the victim to enter or update personal information at a phony website that mimics an established, legitimate website which the victim either has used before or perceives to be a safe place to enter information." *Patco Constr. Co., Inc. v. People's United Bank*, 684 F.3d 197, 204 n.5 (1st Cir. 2012). Phishing schemes "are of particular concern to the elderly." Eric L. Carlson, *Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow*, 14 Elder L.J. 423, 435 (2006).

Most significantly, because "very little [personal] information is required to obtain credit, an identity thief can open numerous fraudulent accounts with information as basic as a social security number matched with an approximate name and birth date." Eric T. Glynn, *The Credit Industry and Identity Theft: How to End an Enabling Relationship*, 61 Buffalo L. Rev. 215, 223 (2013). In such instances, victims "can spend years trying to resolve bad debt run up by thieves in

their names."[8] In 2009, identity fraud victims spent an average of 21 hours and approximately $373 to resolve such fraud. Fitterer, 9 Nw. J. Tech. & Intellectual Prop. at 7 (citing Javelin Strategy & Research, *2010 Identity Fraud Survey Report: Consumer Version* 5 (2010)). The costs of resolving identity fraud affect lower-income people disproportionately, with consumers earning less than $15,000 annually spending twice the amount of time and money addressing credit issues as consumers earning more than $150,000 per year.[9]

On top of the expenditure of time and financial resources necessary to resolve a fraud dispute, the fall-out from a damaged credit report can be devastating. Victims of identity fraud may be denied loans for housing or education or lose employment opportunities, Glynn, 61 Buffalo L. Rev. at 225, be unable to rent an apartment,[10] pay higher car insurance premiums,[11] or be able to access sources of credit only at higher interest rates.[12] The ramifications are not solely pecuniary, as the emotional distress caused by a damaged credit history can

[8] Anderson, *Identity Theft Growing, Costly to Victims*, *supra* n.3.
[9] Consumers Union, *Fact Sheet About ID Theft*, http://www.defendyourdollars.org/pdf/defendyourdollars.org-fact_sheet_about_ id_theft.pdf.
[10] *See* Experian, *Identity Theft Impact on Credit Score*, http://www.protectmyid.com/identity-theft-protection-resources/identity-basics/ credit-score-impact.aspx.
[11] *Id.*
[12] *Id.*

be severe.[13] Even worse, because there may be a considerable delay between the occurrence of a corporate data breach and the point at which that data is misused to the detriment of the consumer, and between the first date of misuse and the date of discovery,[14] consumer injury following a data breach is very difficult if not impossible to avoid.

Defendants' argument that the theft of data does not result in substantial injury to consumers because federal law limits a consumer's liability for, and requires credit card issuers to rescind, unauthorized charges, Def. Wyndham Hotels & Resorts LLC's (Hotels) Br. 19-20 (citing 15 U.S.C. § 1643(a)(1)(B)), wholly ignores the harms—pecuniary and otherwise—attendant with the unauthorized use of consumers' personal data. Consumers incur harm in the form of time and expenses spent disputing fraudulent charges or repairing a credit report; in some cases, they may pay fraudulent charges to clear their credit reports. Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & Tech. 2, at *23 (2009). In

[13] Janine Benner, Beth Givens, & Ed Mierzwinski, *Nowhere to Turn: Victims Speak Out on Identity Theft*, May 1, 2000, https://www.privacyrights.org/ar/idtheft2000.htm; *see also* Fitterer, 9 Nw. J. of Tech. and Intellectual Prop. at 10.

[14] *See, e.g.*, FTC, *2006 Identity Theft Survey Report* 23 (2007) (indicating that one-quarter of victims of existing credit card fraud in one survey did not discover misuse for more than one month after the date of the first misuse and that three percent did not discover the misuse for six months or more).

addition, consumers suffer damage to credit history (and the corresponding harms flowing from that damage) and emotional distress.[15]

Moreover, defendants' reliance on *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), for the argument that no substantial consumer injury occurred in this case is inapposite. In *Reilly*, the Third Circuit affirmed dismissal of the plaintiffs' claims on the grounds that plaintiffs had not alleged that a hacker had used their financial information to make unauthorized purchases and thus had not suffered an injury-in-fact. 664 F.3d at 42. Here, the complaint makes clear that at least some of the information stolen during the three data breach incidents was used subsequently to make unauthorized purchases. *See* First Am. Compl. ¶ 34 ("In May 2009, [d]efendants learned that several Wyndham-branded hotels had received complaints from consumers about fraudulent charges made to their payment card accounts after using those cards to pay for stays at Wyndham-branded hotels."); ¶ 38 ("Again, [d]efendants did not detect this intrusion themselves, but rather learned of the breach from a credit card issuer … [who] indicated that the account

[15] Nor is the brunt of identity fraud borne solely by consumers. The Treasury Inspector General for Tax Administration estimates that the Internal Revenue Service will pay "as much as $21 billion in fraudulent tax refunds over the next five years as a direct result of" identity fraud. *Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part 4*: *Hearing Before the Subcomm. on Government Organization, Efficiency and Financial Management of the H. Comm. on Oversight and Government Reform*, 112th Cong. 2 (2012) (statement of Rep. Platts, Chairman, House Subcomm. on Government Organization, Efficiency and Financial Management).

numbers of credit cards it had issued were used fraudulently shortly after its customers used their credit cards to pay for stays at Wyndham-branded hotels.").

Defendants assert, without any factual support, that they were victimized by the breaches of their systems because they "lost millions of dollars and suffered significant reputational harm when cybercriminals attacked [their] network." Def. Hotels' Br. 21 (emphasis omitted). That argument is irrelevant to whether the FTC may enforce its statutory mandate to police unfair or deceptive corporate practices that are likely to cause substantial injuries to consumers. In any event, although businesses lose "an estimated $150 to $250 for each card number stolen … in the form of legal settlements, fees for consultants hired to remove malware, and personnel hours spent notifying customers … [these] costs are passed on to consumers in the form of higher retail prices and credit-card fees."[16]

Because the theft of consumer data obtained in a data breach is likely to, and often does, cause substantial harm to consumers, this Court should deny defendants' motions to dismiss.

[16] Anderson, *Identity Theft Growing, Costly to Victims*, *supra* n.3.

II. FTC ENFORCEMENT ACTIONS CURRENTLY PROVIDE THE MOST EFFECTIVE MECHANISM TO REDRESS UNFAIR DATA SECURITY PRACTICES THAT RESULT IN BREACHES OF CORPORATE COMPUTER NETWORKS.

FTC enforcement proceedings pursuant to 15 U.S.C. § 45 both deter and redress inadequate corporate data security practices. Notwithstanding that a data breach of a corporate computer system can and does result in substantial injuries to consumers, several federal courts, including the Third Circuit, have held that consumers whose information has been stolen but not (yet) misused either lack standing to bring claims against companies that failed to adequately protect their information or otherwise fail to state a claim. *See, e.g.*, *Reilly*, 664 F.3d at 45 (holding that, without alleging misuse of information, plaintiffs lacked standing because their "credit card statements are exactly the same today as they would have been had [the corporate] database never been hacked"); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (dismissing case because pleading damages for credit monitoring services insufficient to state breach of contract and negligence claims against bank that failed to secure consumer data where consumers had not suffered financial loss to their accounts or been victims of identity theft); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-cv-6060, 2010 WL 2643307, at *2, *7 (S.D.N.Y. June 25, 2010) (dismissing common-law and statutory consumer protection claims for lack of standing where only injury alleged was increased risk of identity theft); *Allison v. Aetna, Inc.*, No. 09-cv-2560, 2010

WL 3719243, at *4 n.3 (E.D. Pa. Mar. 9, 2010) (collecting cases finding no standing); *Hinton v. Heartland Payment Sys., Inc.*, No. 09-cv-594, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (finding that plaintiff failed to plead an actual injury because data had not been misused).

Perhaps because of the absence of a private enforcement mechanism to date, "[m]ost merchants are content to clean up the damage from an attack, rather than pay for better preventive measures."[17] Administrative enforcement by the FTC is therefore necessary to protect consumers, as it prompts companies to take adequate measures to secure their computer systems and to safeguard consumer information. It also serves as a critical remedial backstop while private challenges to consumer data breaches mature and while injuries underlying private claims develop.

The FTC has used its authority to bring data security cases for more than a decade, and it has settled cases involving conduct similar to that in this case. In 2005, the FTC settled an enforcement action against BJ's Wholesale Club (BJ's) following allegations that BJ's maintained unfair practices by failing to take reasonable and appropriate security measures to protect the consumer information—including names, credit and debit card numbers, and expiration dates—it transmitted through its in-store and central computer networks to obtain

[17] Anderson, *Identity Theft Growing, Costly to Victims*, *supra* n.3.

and receive payment authorizations from issuing banks.[18] Similar to the allegations in this case, BJ's failed to encrypt the consumer information it transmitted, allowed anonymous access to the information through the use of default user ids and passwords, and failed to maintain adequate measures that would detect unauthorized access on its networks.[19] As a result, hackers were able to obtain consumers' debit and credit card numbers, which were then encoded onto counterfeit cards used to make several million dollars in fraudulent purchases.[20] Because the card issuers were forced to cancel the cards to prevent further fraudulent use, those consumers were prevented from making purchases using credit or accessing their bank accounts.[21] The FTC's settlement with BJ's required the company, among other things, to design and implement a "comprehensive information security program … reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers," and to retain an independent auditor to certify its compliance with the settlement.[22] These measures offer strong protection for consumer data.

---

[18] FTC Administrative Complaint ¶¶ 4-5, 9-10, *In the Matter of BJ's Wholesale Club, Inc.*, http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.
[19] *Id.* ¶ 7.
[20] *Id.* ¶ 8.
[21] *Id.*
[22] FTC Decision and Order at 2-3, *In the Matter of BJ's Wholesale Club, Inc.*, http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

Similarly, the FTC brought an enforcement action against Dave & Buster's, Inc. in 2010 for failing to take reasonable and appropriate measures to protect customers' credit and debit card information stored on the company's in-store and corporate computer networks.[23] Of particular relevance to this case, the FTC alleged that Dave & Buster's failed to employ an intrusion detection system and monitor its system logs for unauthorized access, failed to adequately restrict third-party access to its networks by either granting temporary access or limiting access to certain IP addresses, and failed to employ firewalls or other measures that would have limited access to the payment card information on each in-store network.[24] These failures resulted in a data breach in which approximately 130,000 credit and debit cards were compromised.[25] Some of this information was used to make approximately several hundred thousand dollars in fraudulent transactions.[26] The FTC settled its complaint against Dave & Buster's on terms similar to its agreement with BJ's, requiring the implementation and maintenance of a data

[23] FTC Administrative Complaint ¶¶ 4-5, 10-11, *In the Matter of Dave & Buster's, Inc.*, http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf.
[24] *Id.* ¶ 7.
[25] *Id.* ¶ 9.
[26] *Id.*

security system reasonably designed to safeguard consumer information, periodic audits of that system, and retention of documentation of its compliance efforts.[27]

In the FTC's 2011 enforcement action against Statewide Credit Services (Statewide), a consolidator of credit reports issued by the three major credit reporting agencies, the FTC alleged violations of several consumer protection statutes, including Section 5 of the FTC Act.[28] Of particular relevance here, Statewide allowed its end users, usually mortgage brokers who purchased the consolidated reports, to access those reports through Statewide's portal even though some of them did not maintain adequate data security protocols, such as firewalls or updated antivirus software.[29] Although the computer networks of Statewide and its end users were breached multiple times over a 13-month period, resulting in unauthorized access of 323 consolidated consumer reports, Statewide failed to make any efforts to identify and repair any vulnerabilities in its systems.[30] As with its agreements with BJ's and Dave & Buster's, the FTC's settlement with Statewide required the establishment of data security practices aimed at, among

---

[27] FTC Decision and Order at 2-4, *In the Matter of Dave & Buster's, Inc.*, http://www.ftc.gov/os/caselist/0823153/100608 davebustersdo.pdf.
[28] FTC Administrative Complaint ¶¶ 4, 13-19, *In the Matter of Fajilan & Assoc., Inc. d/b/a Statewide Credit Services*, http://ftc.gov/os/caselist/0923089/110819 statewidecmpt.pdf.
[29] *Id.* ¶¶ 5, 7-9.
[30] *Id.* ¶¶ 10-12.

other things, the "prevention, detection, and response to attacks, intrusions, or other system failures" to protect against theft of consumer information.[31]

FTC enforcement actions such as these are necessary to address the market failure presented by companies that fail to take reasonable measures to protect consumer data on their systems and to prevent future substantial injury to consumers that is likely to result from a data breach incident.

CONCLUSION

For the foregoing reasons, and for those stated in the FTC's opposition brief, the Court should deny defendants' motions to dismiss.

Dated: May 28, 2013

Respectfully submitted,

s/ Jehan A. Patterson
Jehan A. Patterson
Julie A. Murray
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
Tel: (202) 588-1000
jpatterson@citizen.org

Attorneys for Amici Curiae Public Citizen, Inc. and Chris Jay Hoofnagle

[31] FTC Decision and Order at 3, *In the Matter of Fajilan & Assoc., Inc. d/b/a Statewide Credit Services*, http://ftc.gov/os/caselist/0923089/110819statewidedo.pdf.